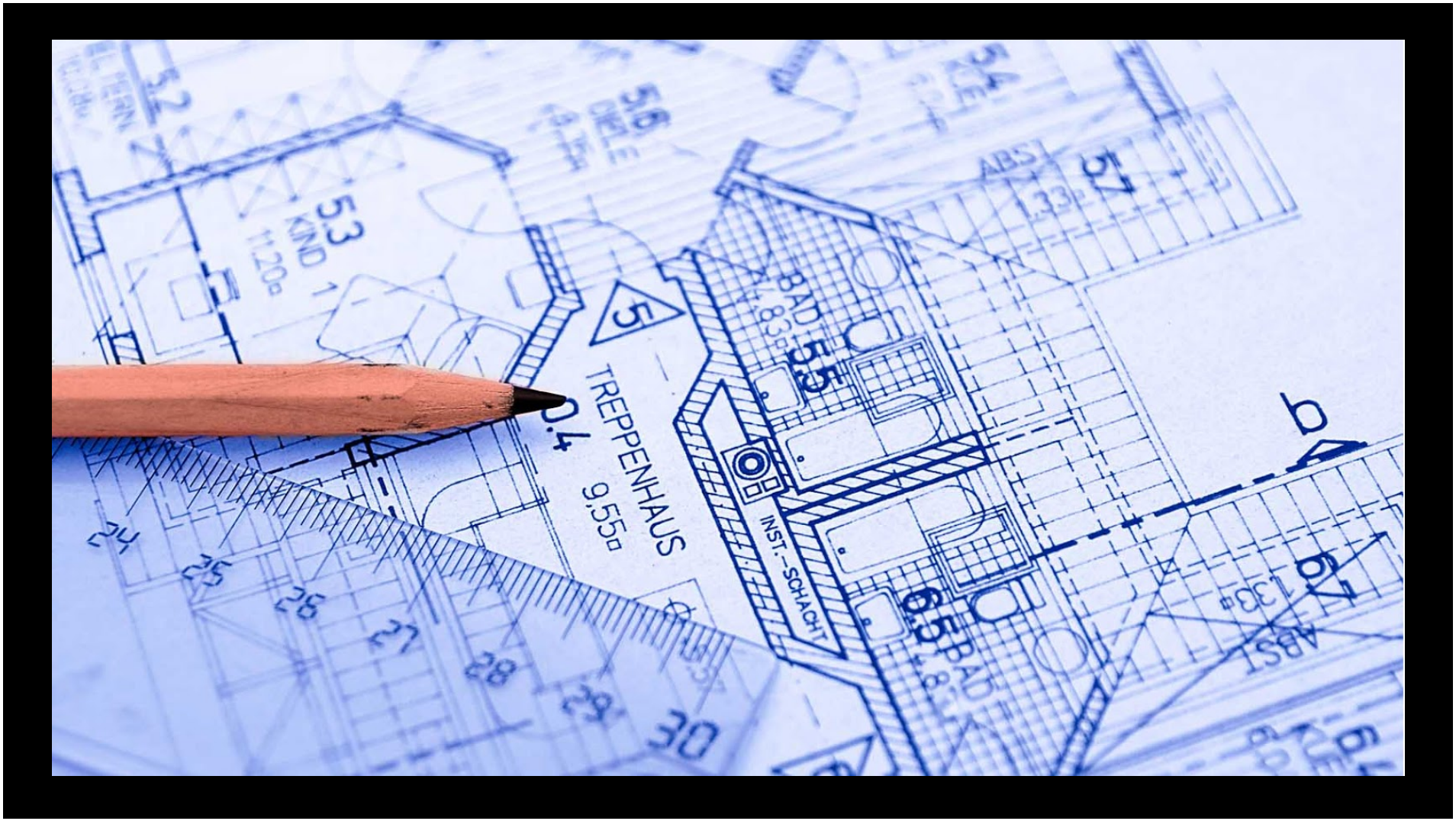
Practical Steps Taken to Reboot Vulnerability Management for Modern IT and Mature Business

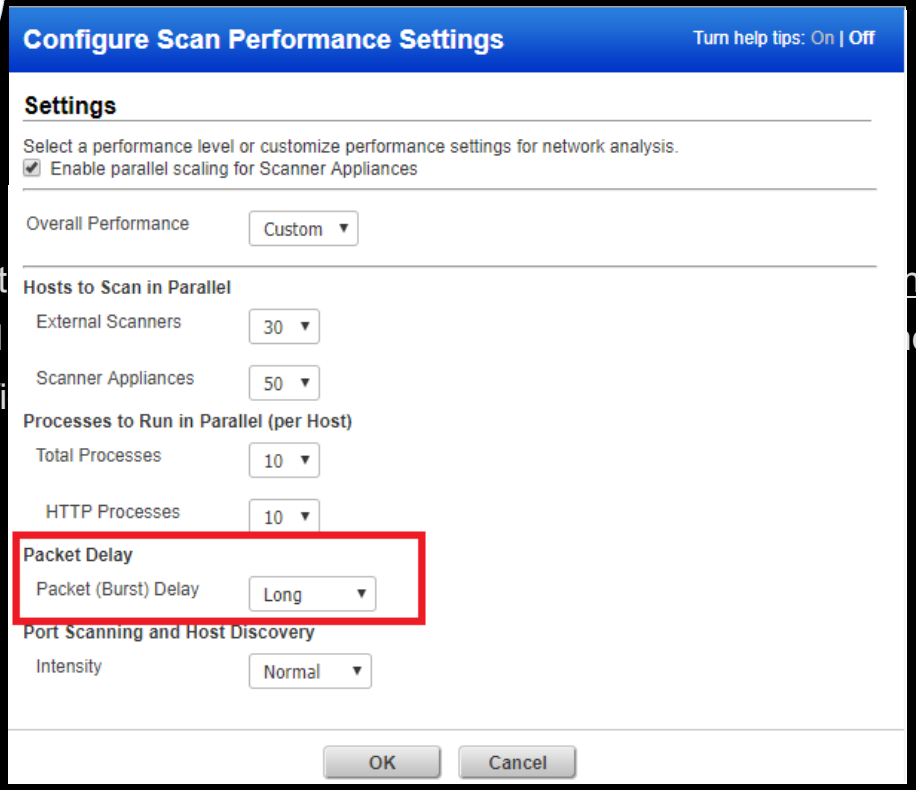
Brian Canaday
IT Security Analyst/Engineer
CSAA, Insurance Group a AAA Insurer

Key Talking Points

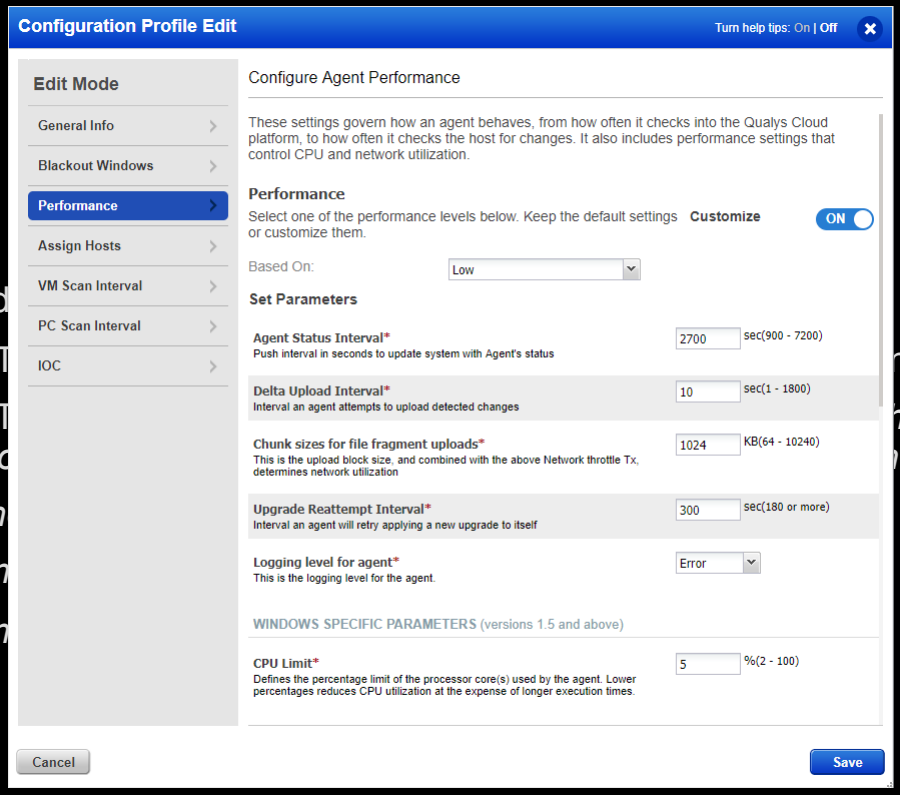
- A Three-Phase Approach to Meeting our Vulnerability Management Goals with Qualys
- Scan Configurations & Schedule Tuning
- Cloud Agent Configuration & Testing with Application Teams

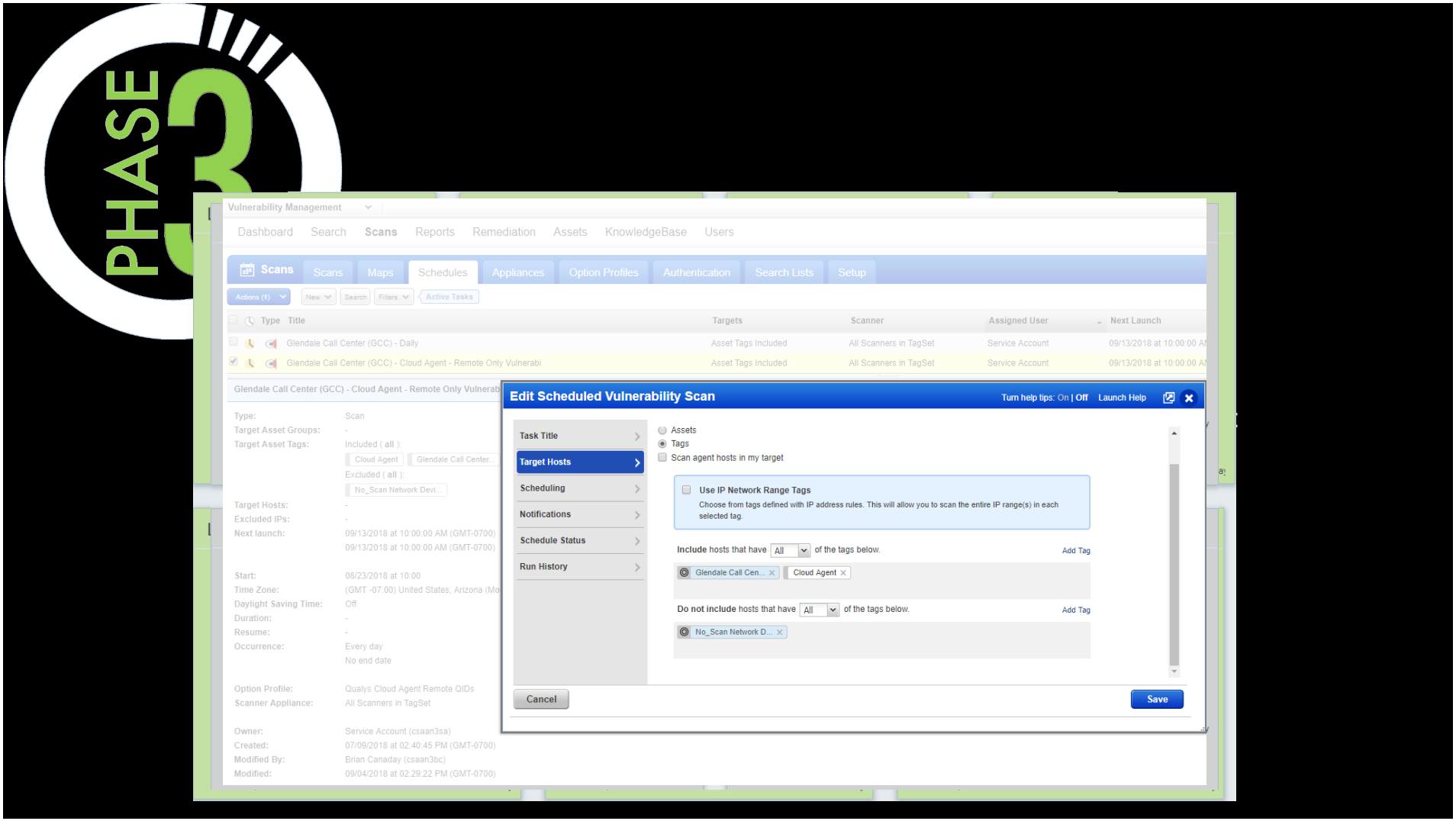

TREPPENHAUS
9,55
INST.-SCHACHT
BAD
ABS

1. What nment
2. Build ces
3. Confi



1. Plan and
2. Identify T ng the Agent
3. Identify T *hose to Work*
   With all c the Agent.
4. *Test, Tun*
5. *Deploy in*
6. *Deploy in*



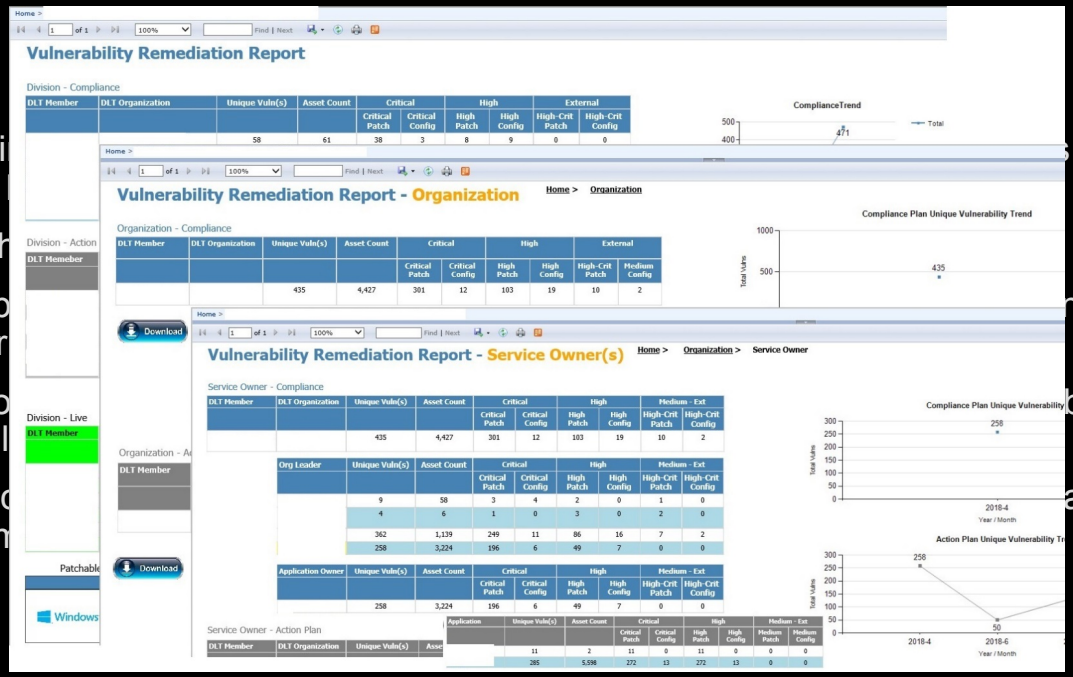

PHASE 3
Vulnerability Management
Dashboard
Search
Scans
Reports
Remediation
Assets
KnowledgeBase
Users
Scans
Scans
Maps
Schedules
Appliances
Option Profiles
Authentication
Search Lists
Setup
Actions (1)
New
Search
Filters
Active Tasks
Type
Title
Targets
Scanner
Assigned User
Next Launch
Glendale Call Center (GCC) - Daily
Asset Tags Included
All Scanners in TagSet
Service Account
09/13/2018 at 10:00:00 AM
Glendale Call Center (GCC) - Cloud Agent - Remote Only Vulnerabi
Asset Tags Included
All Scanners in TagSet
Service Account
09/13/2018 at 10:00:00 AM
Glendale Call Center (GCC) - Cloud Agent - Remote Only Vulnerabi
Type: Scan
Target Asset Groups: -
Target Asset Tags: Included (all):
Cloud Agent
Glendale Call Center...
Excluded (all):
No_Scan Network Devi...
Target Hosts: -
Excluded IPs: -
Next launch: 09/13/2018 at 10:00:00 AM (GMT-0700)
09/13/2018 at 10:00:00 AM (GMT-0700)
Start: 08/23/2018 at 10:00
Time Zone: (GMT -07:00) United States, Arizona (Mo
Daylight Saving Time: Off
Duration: -
Resume: -
Occurrence: Every day
No end date
Option Profile: Qualys Cloud Agent Remote QIDs
Scanner Appliance: All Scanners in TagSet
Owner: Service Account (csaan3sa)
Created: 07/09/2018 at 02:40:45 PM (GMT-0700)
Modified By: Brian Canaday (csaan3bc)
Modified: 09/04/2018 at 02:29:22 PM (GMT-0700)
Edit Scheduled Vulnerability Scan
Turn help tips: On | Off
Launch Help
Task Title
Target Hosts
Scheduling
Notifications
Schedule Status
Run History
Assets
Tags
Scan agent hosts in my target
Use IP Network Range Tags
Choose from tags defined with IP address rules. This will allow you to scan the entire IP range(s) in each selected tag.
Include hosts that have All of the tags below.
Add Tag
Glendale Call Cen...
Cloud Agent
Do not include hosts that have All of the tags below.
Add Tag
No_Scan Network D...
Cancel
Save

Reporting - Better Data, Better Results

- Utilizi… Every Four …

With Th…

1. App… nly Items Our…
2. Sho… bility to Drill…
3. Trac… aging the San…



Outcomes

- With cleaner more relevant data we can detect changes in our environment sooner
- With faster results and less impact on the systems the Qualys Cloud Agent has quickly become the one security agent our Operations Teams depend on and expect immediate remediation of any agent not reporting in
- By leveraging the API from Qualys and our CMDB we use a custom reporting solution where we rollup under the VP for each area and the leaders under them

Questions